CLAIMS

What is claimed is:

Sub a'

1. A method for securely providing information comprising the steps of:

(a) receiving information identifying an encrypted personal security device;

(b) providing said identified encrypted personal security device;

(c) receiving authentication information; and

(d) providing decryption information for said personal security device responsive to said authentication information.

2. The method of claim 1 wherein steps (a) and (b) comprise:

(a) receiving information identifying an encrypted key; and

(b) providing said identified encrypted key.

3. The method of claim 1 wherein step (a) comprises receiving information identifying an encrypted personal security device, the personal security device comprising information necessary to make a secure network connection between a network client and a network server.

4. The method of claim 1 wherein step (a) comprises receiving information identifying an encrypted personal security device, the personal security device comprising information necessary to make a secure virtual private network connection.

5. The method of claim 1 further comprising the step of validating said authentication information.

6. The method of claim 1 wherein step (b) further comprises the steps of:

(b-a) retrieving said personal security device; and

(b-b) providing said personal security device.

7. The method of claim 6 wherein step (b-a) comprises retrieving said personal security device from an authentication server.

8. The method of claim 1 further comprising the step of storing said personal security device on a smartcard.

9. The method of claim 1 further comprising the step of storing said decryption information in a volatile memory element.

10. The method of claim 1 wherein step (c) comprises receiving time-dependent authentication information.

11. A method for accessing secure information comprising the steps of:

(a) receiving an encrypted personal security device;

(b) receiving decryption information for said personal security device; and

(c) decrypting said personal security device.

12. The method of claim 11 further comprising the step of using said decrypted personal security device to access said secure information.

13. The method of claim 11 wherein receiving step (a) comprises receiving an encrypted personal security device comprising information necessary to make a secure network connection between a network client and a network server.

14. The method of claim 11 wherein receiving step (a) comprises receiving an encrypted personal security device comprising information necessary to make a secure virtual private network connection.

15. The method of claim 11 further comprising the steps of:

(d) transmitting information identifying an encrypted personal security device; and

(e) transmitting authentication information.

16. The method of claim 15 wherein step (e) comprises transmitting time-dependent authentication information.

17. The method of claim 11 further comprising the step of storing said personal security device on a smartcard.

18. The method of claim 11 further comprising the step of storing said decryption information in a volatile memory element.

19. A method for allowing a network client secure access to information, the method comprising the steps of:

(a) requesting, by said network client, a personal security device from a network server, wherein said personal security device comprises encrypted information necessary to make a secure network connection;

(b) forwarding, by said network server, said personal security device to said network client; and

(c) providing, by said network server, decryption information for said personal security device.

20. The method of claim 19 wherein step (b) comprises providing an encrypted personal security device comprising information necessary to make a secure virtual private network connection.

21. The method of claim 19 further comprising the steps of:

(d) forwarding, by said network server said request to an authentication server;

(e) querying, by said authentication server a user database with said request;

(f) returning, by said user database a personal security device to said authentication server; and

(g) forwarding, by said authentication server said personal security device to said network server.

22. The method of claim 19 further comprising the steps of:

(h) obtaining, by said client, authentication information from an authentication token;

(i) providing, by said client, said authentication information to said authentication server;

(j) confirming, by said authentication server, the validity of said authentication information;

(k) retrieving, by said network server, decryption information for said personal security device from a database; and

(l) providing, by said network server, decryption information for said personal security device to said client.

23. The method of claim 22 wherein step (h) comprises obtaining time-dependent authentication information.

24. The method of claim 19 further comprising the steps of:

(m) decrypting, by said client, said personal security device.

25. A device for providing secure access to information comprising:

(a) a first receiver receiving information identifying an encrypted personal security device;

(b) a first transmitter providing said identified personal security device;

(c) a second receiver receiving authentication information; and

(d) a second transmitter providing decryption information for said personal security device responsive to said authentication information.

26. The device of claim 25 wherein said receiver receives said encrypted personal security device comprising an encrypted key.

27. The device of claim 25 wherein said receiver receives said encrypted personal security device comprising information necessary to make a secure network connection between a network client and a network server.

28. The device of claim 25 wherein said receiver receives said encrypted personal security device comprising information necessary to make a secure virtual private network connection.

29. The device of claim 25 further comprising an authenticator validating said authentication information.

30. The device of claim 25 wherein said first receiver is the same as said second receiver.

31. The device of claim 25 wherein said first transmitter is the same as said second transmitter.

32. The device of claim 25 wherein said authentication information is time-dependent.

33. A device for accessing secure information comprising:

(a) a first receiver receiving an encrypted personal security device;

(b) a second receiver receiving decryption information for said personal security device; and

(c) a decryptor decrypting said personal security device.

34. The device of claim 33 wherein said receiver receives said encrypted personal security device comprising information necessary to make a secure network connection between a network client and a network server.

35. The device of claim 33 wherein said receiver receives said encrypted personal security device comprising information necessary to make a secure virtual private network connection.

36. The device of claim 33 further comprising:

(d) a first transmitter transmitting information identifying an encrypted personal security device; and

(e) a second transmitter transmitting authentication information.

37. The device of claim 36 wherein said first transmitter is the same as said second transmitter.

38. The device of claim 36 wherein said authentication information is time-dependent.

39. The device of claim 33 further comprising a smartcard storing said decryption information.

40. The device of claim 33 further comprising a volatile memory element storing said decryption information.

41. The device of claim 33 wherein said first receiver is the same as said second receiver.

42. A system for providing secure access to information comprising:

(a) a network client comprising a volatile memory element; and

(b) a network server storing an encrypted personal security device in a server memory element, said personal security device comprising encrypted information.

43. The system of claim 42 further comprising a smartcard having a volatile memory element storing said personal security device.

44. The system of claim 42 wherein said user database includes said personal security device.

45. The system of claim 42 further comprising decrypted information for forming a secure network connection between said client and said server wherein said decrypted information is derived from applying said decryption information to said personal security device.

46. The system of claim 42 wherein said decryption information is stored in said volatile storage.

47. The system of claim 42 wherein said decrypted information is stored in said volatile storage.

48. The system of claim 42 wherein said network is a virtual private network.

49. The system of claim 42 wherein said encrypted information comprises information necessary for forming a secure network connection between said client and said server.

50. The system of claim 42 further comprising:

(c) an authentication token, wherein said token is capable of providing authentication information; and

(d) an authentication server, wherein said authentication server comprises a user database, wherein said user database comprises decryption information for said personal security device, and wherein said authentication server is capable of providing said decryption information upon receipt of said authentication information.

51. The system of claim 50 wherein said authentication information is time-dependent.